State of Iowa Enterprise Removable Storage Encryption Standard

February 14, 2008

Purpose
This standard establishes minimum requirements for the encryption of removable storage devices and media including USB flash drives, portable hard disks, CDs, DVDs, floppy disks and others, to protect State data resources.

Overview
Removable storage devices and media allow portability of data and programs. They are easy to use, inexpensive, small, and capable of holding large quantities of data. These same characteristics present security concerns. Their small size makes them easy to lose or steal. Their portability promotes removal of data from secure systems for use away from the office.

This standard identifies steps that must be taken to ameliorate the risks associated with the use of removable storage devices and media.

Scope
This standard sets minimum requirements for encryption of data on removable storage devices. This standard does not apply to files written to tape or other media as part of an agency's regular backup process when the software being used is intended solely for the purpose of creating and managing backups.

This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise level policies, standards, guidelines, processes and procedures.

Definitions
Selected terms used in the Enterprise Removable Storage Data Protection Standard are defined below:

- **Encryption:** The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).

- **Removable Storage:** Devices and media to which electronic information can be copied and which can be easily removed from one computer and used on another.

Enterprise Removable Media Encryption Standard

The following minimum standards must be met for all forms of removable storage devices and media:

1. **Policy:** Agencies shall establish a policy covering the use of removable storage devices and media. At a minimum the policy shall cover:
    a. The types of data permitted on removable storage devices and media.
    b. The types of devices permitted.
    c. Reporting of lost or stolen devices.

2. **Data Encryption:** Confidential data stored on removable storage devices and media must be encrypted.

    • The encryption shall be with the Advanced Encryption Standard (AES[i]) cipher using at least a 256-bit key length.
    • A strong pass phrase for accessing encrypted data must be used; at least 8 characters, a mix of numbers and letters with at least one special character.
    • The encryption process shall be centrally managed at the agency and/or enterprise level.

3. **Physical Protection:** Users of removable storage devices and media are responsible for their physical protection.

4. **Primary Storage/Data Backups:** To ensure data availability in the event of device loss or theft, removable storage devices and media should not be the primary storage device for any State of Iowa data. If removable storage devices and media are primary storage for critical data, frequent and regular backups of the data should occur according to agency policy.

5. **Assessment:** The ISO will periodically assess agency compliance with this standard. Agencies will provide access to inventory information and systems as required to determine compliance. If violations of this standard are identified, the agency will receive written notification pursuant to IAC 11--25.11(8A).

6. **Awareness Training:** Staff shall be provided with removable storage device and media security awareness training. At a minimum, users shall be provided with documentation describing removable storage devices and media risks.

Effective Date
Agencies must be fully compliant with this standard no later than March 31, 2008. However, agencies are encouraged to implement this standard as soon as possible to protect critical data assets.

Enforcement
This standard will be enforced per IAC 11--25.11(8A). The Information Security Office will periodically assess a random sampling of removable storage devices and media in use by agencies to assure the devices and media are properly encrypted.

---

[i] Prior to its adoption by NIST in 2000 with the issuance of FIPS 197, AES was commonly known as the Rijndael block cipher.